GeekBrains

Урок 3 Тема 2

Процесс загрузки PE-файлов

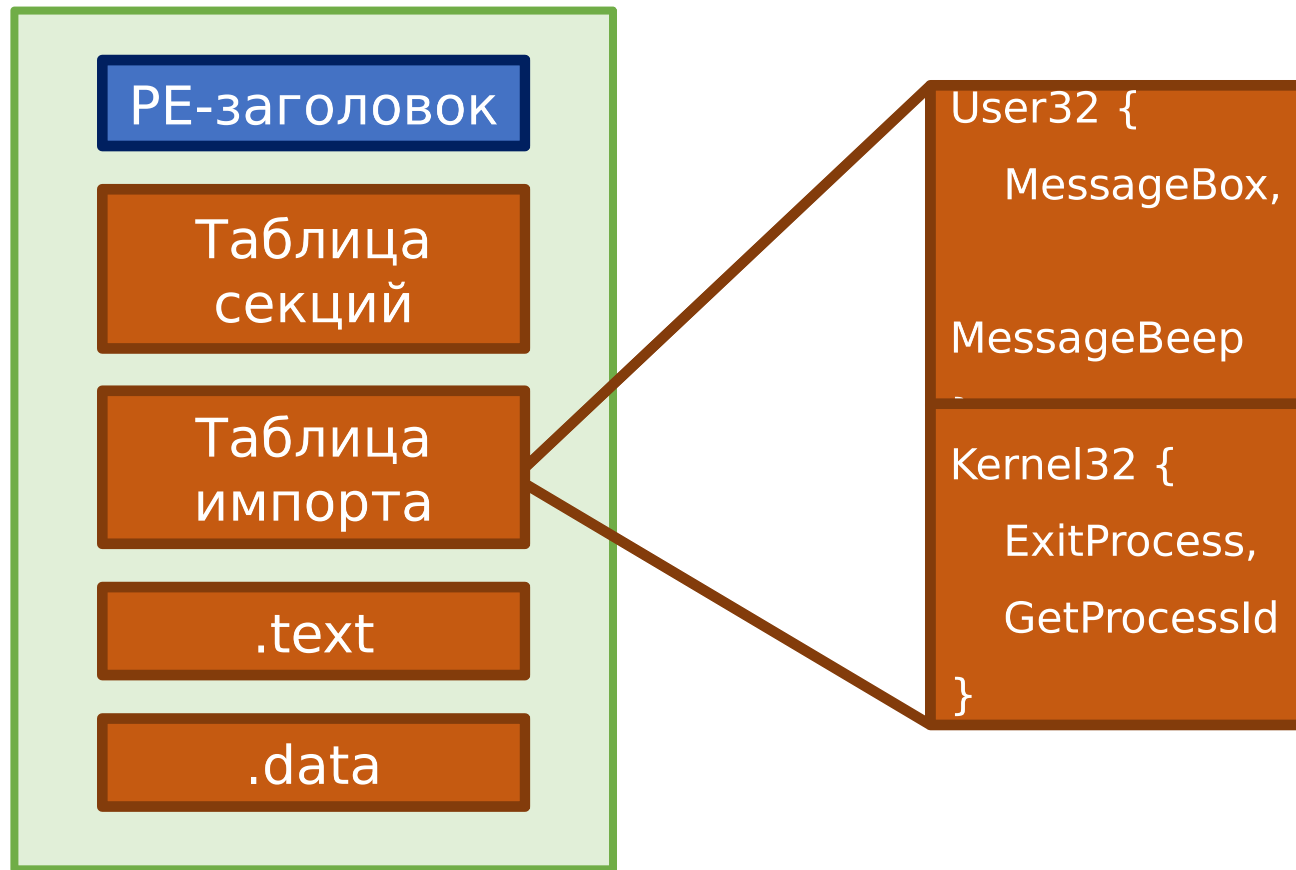
Реверс-инжиниринг

В этом видео

1. Алгоритм вычисления RVA важных структур данных.
2. Структура таблицы импорта.
3. Структура таблицы экспорта.
4. Основные этапы загрузки PE-файла.

GeekBrains

Общая структура PE-файла



GeekBrains

Алгоритм вычисления RVA таблицы импорта

DATA_DIRECTORY
    ...
    > DIRECTORY_ENTRY_IMPORT
        Name RVA
        Name
        OriginalFirstThunk
        ...
        FirstThunk
    ...
    > DIRECTORY_ENTRY_IAT
        struct IMPORT_ADDRESS_TABLE

Структура таблицы импорта

```
DIRECTORY_ENTRY_IMPORT
    struct IMPORT_DESCRIPTOR
    {
        OriginalFirstThunk // Import Lookup Table RVA
        Time/Date Stamp
        Forwarder Chain
        Name RVA           // например, kernel32.dll
        FirstThunk         // Import Address Table RVA
    }
```

GeekBrains

Описание структуры IMAGE_IMPORT_BY_NAME

```
struct IMAGE_IMPORT_BY_NAME
{
    Hint
    Name1 // например, ExitProcess
}
```

GeekBrains

Структура таблицы экспорта

```
DATA_DIRECTORY
    > DIRECTORY_ENTRY_EXPORT
        struct IMAGE_EXPORT_DIRECTORY
        {
            ...
            NumberOfFunctions
            ...
            AddressOfFunctions
            AddressOfNames
            AddressOfNameOrdinals
        }
```

Основные этапы загрузки PE-файла

1. Проверка PE-файл на корректность.
2. Поиск RVA PE-заголовка в DOS-заголовке.
3. Анализ PE-заголовка.
4. Копирование PE-файла в виртуальную память.
5. Анализ таблицы импорта.
6. Копирование динамических библиотек в виртуальную память.
7. Анализ таблицы экспорта.
8. Коррекция адресов в основной программе.
9. Передача управления на точку входа.

Итоги

1. Узнали алгоритм вычисления RVA важных структур данных.
2. Познакомились со структурой таблиц импорта и экспорта.
3. Разобрали основные этапы загрузки PE-файла.